A Virtualised High Trust Zone (VHTZ) to Mitigate the Security and Privacy Issues in Cloud Computing

Tanveer A Zia[†] and Bhupesh Mansukhani[††],
[†]*tzia@csu.edu.au*
[††]*bhupeshmansukhani@yahoo.com*
Charles Sturt University, School of Computing and Mathematics, NSW, Australia

Summary
The benefits of cloud computing are clearly well known which include rapid deployment, ease of customization, reduce cost and low risks. However, some high profile security breaches confuse organizations as they attempt to deploy cloud services in their businesses. Although, the cloud service providers pitch the security of their services. Enhancements in existing security measures and advanced solutions are needed to ensure high level security and privacy of data on cloud. This paper provides a holistic overview of cloud security issues by encompassing unique threats in cloud computing and presents findings of a survey of practitioners view on cloud security. A Virtualized High Trust Zone (VHTZ) is then presented as a solution, especially for infrastructure based cloud services to tackle the attacks and network monitoring in a virtualized infrastructure.

Key words:
Cloud security, high trust zone, infrastructure as a service, VM threats, network monitoring.

1. Introduction

Due to increasing connectivity and virtualisation cloud computing has become mainstream venture for today's technology savvy enterprises. The main driving forces are elimination of up front capital and reduction in operational expenses. This leads to an increase adoption of cloud computing. However, still many organisations approach cloud computing sceptically. This is primarily because of the security issues associated with allowing a third party to manage data access and storage. To visualise the cloud's security issues, cloud fundamentals need to be understood. There are several definitions of cloud computing, the US National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to shared computing resources, networks, servers, storage, applications and services that can be readily accessible with minimal efforts. In cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other networked devices. Cloud infrastructure can reside within the company's datacenters as internal clouds or on-premise solutions as external cloud computing resources. It encompasses any subscription-based or pay-per-use service that extends existing IT capabilities. Typically, a cloud utilizes a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed. By design, cloud computing is scalable, flexible and elastic – offering IT staffs a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software.

There are three key elements or delivery platforms of cloud computing. Applications running through any of these platforms pose various security privacy challenges. The three cloud delivery platforms are infrastructure as a service (IaaS), Software as a service (Saas), and platform as a service (PaaS). In IaaS cloud provider supplies a set of virtualized infrastructure such as virtual machines (VMs) via remote access and customers can run their applications. SaaS is an enterprise level information based software service, typically available over the public internet. PaaS enables development and programming environment allowing cloud users a runtime environment.

This paper extends our earlier studies 'an empirical study of challenges in managing the security in cloud computing' [1] and 'Security challenges and countermeasures in cloud computing' [2] and provides our holistic approach in securing cloud computing using a High Trust Zone (HTZ) virtual environment.

The HTZ emphasizes on virtual environment in IaaS due to its extensible delivery model which allows abstract infrastructure and resources to be made available to clients as isolated Virtual Machines (VMs) [3].

2. Unique Security and Privacy Issues in Cloud Computing

Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Cloud architectures must have well-defined

security policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for cloud environments and traditional security controls. Cloud computing and its service platforms are exposed to security and privacy issues, mainly due to the fact that the users do not have a control over the data. This raises several questions such as (1) trust, can users trust a cloud service which is open to various vulnerabilities (2) data uncertainty, what happens of the cloud sever crashes, how the data is recovered and what are the disaster recovery procedures, and (3) control over data, how much control a user has over their data which might be stored in an unidentified location. Therefore, it is imperative for providers and users of cloud computing to identify any potential security and privacy breaches within the data centers, however actions have to be different each time the breach happens. For instance, there are no privacy laws as specific to computers or their usage in some countries, whereas in other countries such as United States of America [4] there are legislations concerning privacy hence the situations and the actions have to be different accordingly.

The privacy issue in cloud computing are growing but specifically in the public cloud architecture and exclusively in "on-demand" and "pay-as-you-go" model, which is a shared cloud computing platform and is opted by various enterprises for further cost reduction while opting for cloud computing, most of the providers opt for virtualization being a part of public cloud, as it enables them to share multiple resources with various users in an independent environment, however the virtualization itself is vulnerable to attacks and once attacked opens a pathway to all types of issues pertaining to cloud computing and to the physical host. The following are some high-level privacy issues identified in this paper.

2.1 Minimum User Control

The cloud does offer variety of services and platforms to its users but when it comes to data control the cloud seriously falls flat. Due to very basic reasons that the providers and the users hardly have a control over the data being stored and transmitted as its happening over the cloud and without any strong formed policies at both ends [5]. The moment Software as a Service (SaaS) platform is bought by the user, the cloud service provider automatically engages data storage, however in this case the visibility and control over the data is limited. However users should consider the following key aspects of "minimum user control" before transferring their sensitive data over the cloud.

1. Ownership and control over the infrastructure – The data or the applications over the cloud are processed on the service providers end, hence there is no control over these machines or target platforms by the user, and the possibility of hacking, theft and data misuse can often occur at the providers end, hence the user should consider this aspect very well before moving out all the application control to the cloud at the provider end or make them sign a legal contract which can provide the user with some protection over the misuse of data in any way [6].
2. Access and identity management – It is of serious concern that third party access may be granted to the user data by the provider in some cases such as user data being stored in the data center of the cloud provider somewhere in the USA, according to the US Patriot Act, the legislation and the law enforcement agencies can anytime sneak around the user data whenever they wish to. Hence the user should always make it a point (who owns the data) to ask questions to the service provider as to what access level and transparency levels are provided to the government agencies or to third parties [7].
3. Change of service provider – It is imperative for the user to demand a vendor lock-in on their data while changing the cloud provider due to any reason. The former cloud provider should be locked away from the user data and the user should take charge of the deployment and transferring the applications and data to the new provider.
4. ITIL® practices while reporting privacy breaches or incidents– While selecting the cloud provider, the user should thoroughly go through the incident reporting procedures opted by the provider [7], so in case of a privacy breach or any incident, the same should be reported to the user via official communication channel with the estimated time of resolution and corrective actions.

2.2 Unauthorized Usage of Data

There is possibility that the data stored on the cloud service provider end may be used by third party agencies (besides law enforcement agencies) for advertising purposes, this way the providers can earn extra revenue while sharing the data of the user with the advertising agencies or companies. However there is no such guarantee provided by some service providers that they would not share the user data with third parties but it

should be in the best practices of the user/enterprise to bind the providers in a legal contract agreement clearly mentioning the said point. This will ensure trust between the providers and users and will allow restrained access to their data by third party or advertisers.

2.3 Data Redundancy

Data duplication is one of the benefits of the cloud but is also a point of concern. To protect the data and to take necessary disaster recovery steps the data of the user is replicated over various data centers of the providers, it is difficult to find out genuinely whether all data has been wiped out from the multiple storage locations of the providers (incase such request is made). Definitely the movement of user data increases the complexity of various jurisdictions, legal factors and it can be problematic for the users [8].

Though a lot has changed with respect to privacy, however the areas as described above still need the attention of the cloud service providers and that of the users as well. Only service providers cannot ensure 100% privacy if the users overlook the legal requirements or data redundancy, if the users carry out research before signing a service level agreement with a service provider, it will ensure that service providers and the users a peace of mind.

2.4 Multi Tenancy

Cloud computing users share physical resources with others through common software: virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions [9]. The virtual machine running next to the consumer's environment could be malicious, looking to attack the others or sniff communications moving throughout the system.

2.5 Data Mobility and Control

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, Disaster Recovery or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation such as the US Patriot Act [10] allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners' consent.

2.6 Data Privacy

The public nature of cloud computing poses significant implications to data privacy and confidentiality; Cloud data is often stored in plain text, and only few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly [11]. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on at personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair [12]. Sensitive data stored within cloud environments must be safeguarded to protect its owners and Subjects alike

The risks to cloud computing are further categorized as below:

Unauthorized access – It is always a risk that the data being stored in the cloud can be used by unauthorized personnel's or the third party users especially in "pay-as-you-go" and "on-demand" cloud models where the security of these models are of a least concern to the cloud providers. For instance a virtual machine (VM) on a PaaS service model hosted for a client by a service provider will hardly carry any security checks or security policy updates as that would incur cost and that would be added to the client costs and the service provider might loose the client in added costs to the whole "pay-as-you-go" model and this way they open doors to the attackers.

VM threats – VM threats or virtual machine threats are the most complicated and destructive threats, any loophole or vulnerability in VM can lead the attacker straight to the physical host and thus compromising the physical host. VM threats are on rise these days because the enterprises/users and the cloud service providers do not pay enough attention in updating the VM security policies this can open doors to the attackers inviting them to use the vulnerability and putting everything in the cloud model and the physical host at stake.

Threat Model -The virtualized architecture of cloud computing offers various benefits to the cloud user however security of the cloud is the responsibility that is shared between the cloud user and cloud provider. The users of cloud computing are not aware of the security

policies through which their VMs are protected. On the other side, cloud providers running VMs are not aware of the contents of the VMs. Thus, there is no complete trust between cloud customers and providers. From a cloud provider perspective, the VMs of the user cannot be trusted (due to the unknown applications and various security policies which may or not may be disclosed to the cloud provider). For instance, a hacker can be either a cloud user that may be already hosting a service or a non-cloud user. In either of these models the victim is the cloud provider who runs the service to host the VMs of the users. In case of a security breach, the responsibility and the infrastructure that is compromised belongs to the provider. In the former threat model, hackers have more chances of success due to the fact that they have more access to the cloud computing virtual infrastructure and have the ability to run various malware to gain access on the system.

Security Threats - It is evident that breaching any component of the virtualized cloud infrastructure greatly impacts on the security of the other components and affects the overall security of the cloud computing virtualized infrastructure. [13] investigated several vulnerabilities and threats to the security of the cloud computing especially focusing on the virtualized cloud computing security. These threats can be broadly categorized in three categories:

a) Hypervisor Vulnerabilities - The hypervisor attack is hackers potential target because of only one reason, gaining access to the hypervisor layer will provide access to the underlying layers of the hypervisor and hence will provide access to the hacker on virtual machines installed on the host physical server. If the hypervisor layer is compromised all the virtual machines and their running operating systems and application will come under the attack and hence will breach the security of the entire virtualized environment. Many such attacks have been popular on the hypervisor layer, [14] describe HyperJacking, BluePill and Vitriol and [15] describe SubVir and DKSM as few attacks that can target the virtual layer at the runtime. All these attacks are capable of injecting a malicious hypervisor during the runtime or modifying the existing hypervisor to enable the hacker to gain control over the physical host. However the said was a case of traditional hypervisor attack, in some cases the Xen hypervisor, the hypervisor is not only responsible for administering the Virtual Machines but also controls the other VMs that are running on the same physical host. Imagine a hacker gaining access to the Xen hypervisor will not only control single hosted VMs but multiple VMs running on the same physical host.

b) Virtual Network Layer Vulnerabilities – The virtual network layer or vSwitch layer is also vulnerable to variety of attacks, these attacks can be vSwitch configurations, VLAN's, Trust Zones and ARP tables' corruption. [16] state that vSwitch attacks are not common as they have mostly occurred in the past using a physical network, for instance corrupting the ARP tables of the physical host and then attacking the VMs with a spoofed IP. Hence to attack the vSwitch layer many hackers have to attempt hacking the physical host network layer and if the network layer is vulnerable then the possibility of attacking the vSwitch layer increases.

c) Virtual Machine Vulnerabilities – As it is evident a virtualized cloud infrastructure can contain various VM images and not all of them can be active at once, some of them will be offline and some of them will be online. In either stage whether offline or online they are all prone to serious vulnerabilities. Any attack on the active VM can make the hacker gain access over the physical system however once the VM is compromised, it can be a possibility that the other VMs on the same physical server be compromised too at the same time. According to [17] sharing the same resources increases the risk of attack on other VMs installed on the physical server as all of the VMs installed share the same physical server resources such as memory, hard drives, optical media and hypervisor layer. Having multiple VMs on a single server increases the severity of the damage caused and the risk of VM-to-VM attacks. However if the physical server is in off state, it is safe from any hacker attacks but on the other hand if the VM is offline it is still prone to various attacks as it is available as a virtual image file that can be easily tampered by an internal or external attack, provided the physical server state is on.

3. Practitioners view of Cloud Computing Security

We conducted a survey of 167 people from 40 organisations, resulting in an average of 4-5 personnel per organisation. The survey findings provide some important

information of how practitioners view cloud computing security. Following questions were asked:

1. What cloud services and platforms are used?
2. Who is responsible for ensuring cloud security?
3. Are cloud computing resources evaluated for security prior to deployment?
4. How confident are users about using cloud computing recourses?
5. What are the available technologies that safeguard cloud computing?
6. What information is more risky over the cloud?

In Fig. 1 it is seen that most of the companies and employees are engaged in using cloud computing for critical business applications. As per the survey it was evident that organizations are mainly using SaaS (Software as a service) platform on the cloud to host critical business applications, followed by IaaS (Infrastructure as a service) for hosting infrastructure services on the cloud. Evidently it shows that security on the cloud plays a major concern since most of the organizations are engaged in using cloud for hosting either applications or their infrastructure, compromising security over the cloud will effect these two factor directly.

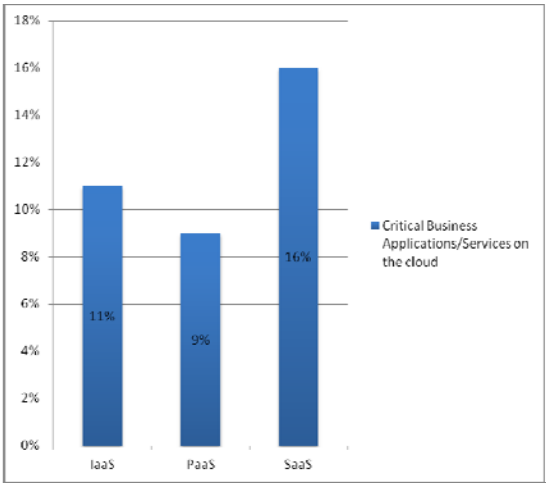

Fig. 1: Critical business applications/services that run on the cloud

As per Fig. 2 most respondents believe that cloud computing providers are responsible for ensuring security on the cloud, over 42% of the respondents believe that service providers are responsible for securing SaaS platforms and 34% of them feel that service providers are responsible for securing the IaaS platform. However the results in Fig. 2 illustrates that organizations are clear in defining the responsibilities of the security of various cloud platforms.

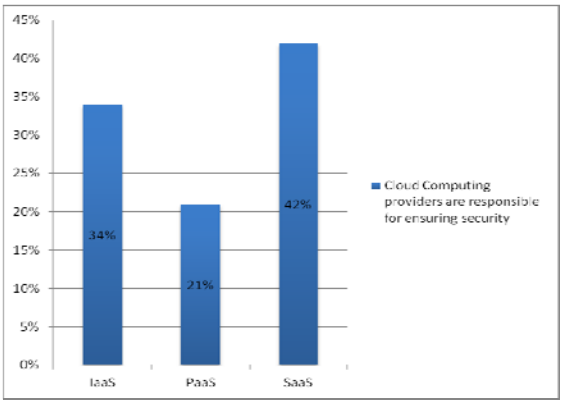

Fig 2: Service providers responsible for ensuring cloud safety

As per Fig. 3 most of the respondents believe that cloud computing resources are not evaluated for security prior to deployment, most security practitioners and network consultants feel that security is not evaluated before deployment over the cloud followed by management in 44% of ratio, hence it seems that all respondents in this category think alike.

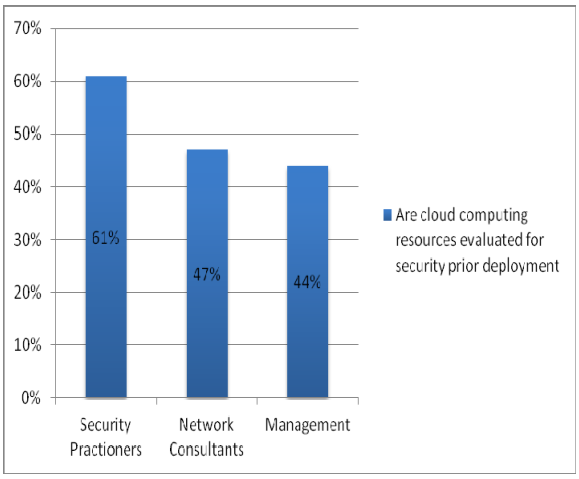

Fig. 3: Evaluation of cloud computing resources prior deployment

Fig. 4 depicts that most of the resources are still under the radar from the respondents' views and knowledge. Especially the management is hardly aware of the new or existing resources that can be used within the cloud with respect to cloud security such as VPN and virtual networks or private clouds. The security practitioners are still aware of the aforesaid technologies and other resources of cloud computing, however the numbers still depict that more knowledge is needed by the respondents on the resources of cloud computing.

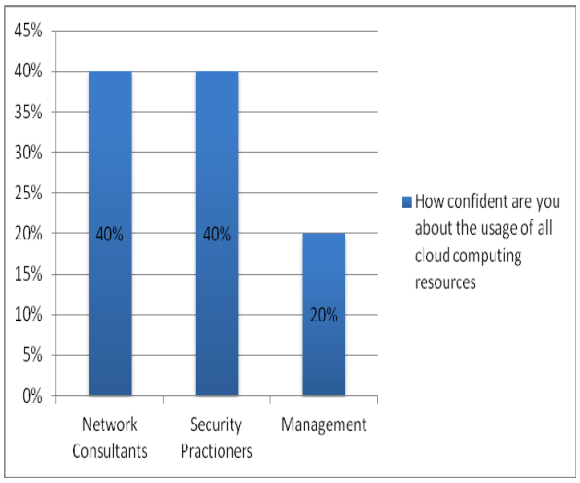

Fig. 4: Usage of cloud computing

Various technologies were listed out to the respondents and their individual responses were recorded on each of the technology to illustrate a combined response. As can been seen in Fig. 5, 70% of the respondents feel SSL certifications and Network Intelligence are best bet for safeguarding cloud computing, followed by VPN and Log Management at the second place.

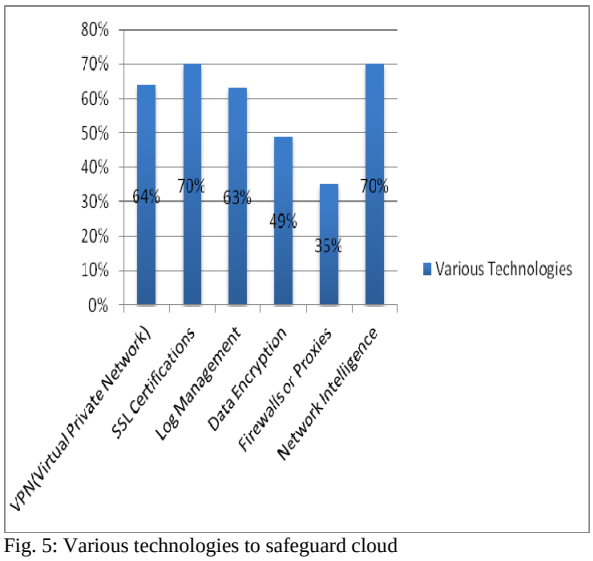

Fig. 5: Various technologies to safeguard cloud

In Fig. 6, the risks were divided in two sections "On-Premise" and "In the cloud", most of the respondents benchmarked "illegal activity" as primary risk to cloud computing, needless to say "illegal activity" refers to hacking, breaking or stealing or all of them with respect to the context of this survey. Followed by security of data assets at second place, this involved the security of data assets at the data centers or IT infrastructure security.

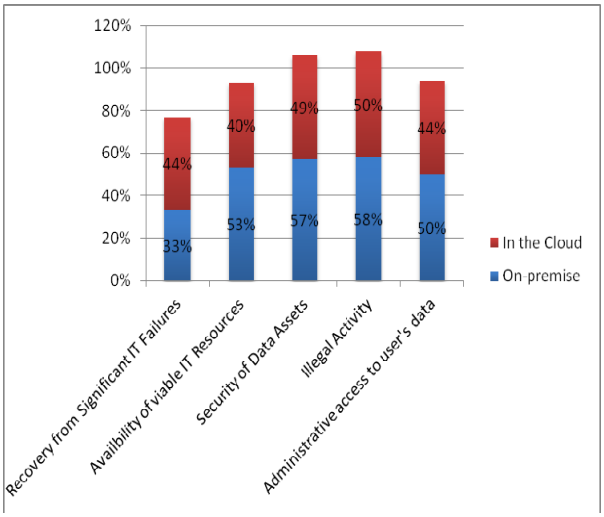

Fig. 6: Identified risks of cloud computing

In Fig. 7 respondents marked out various information categories that can be risky if kept in the cloud, almost 70% people responded with risk of putting intellectual property over the cloud, followed by financial data at 62% and other categories of data were at an average of 40 – 55%, which included credit card information, non-commercial information and employee data.

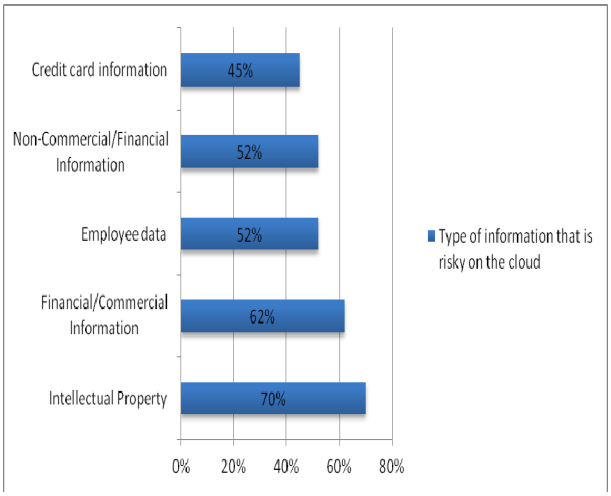

Fig. 7: Information that can be risky on the cloud

4. A Virtualised High Trust Zone (VHTZ)

A High Trust Zone (HTZ) is proposed by [18] to safeguard virtual cloud computing on IaaS platform, and virtual environment. Creating a high trust zone establishes a high degree of trust between the data, users, providers and the systems.

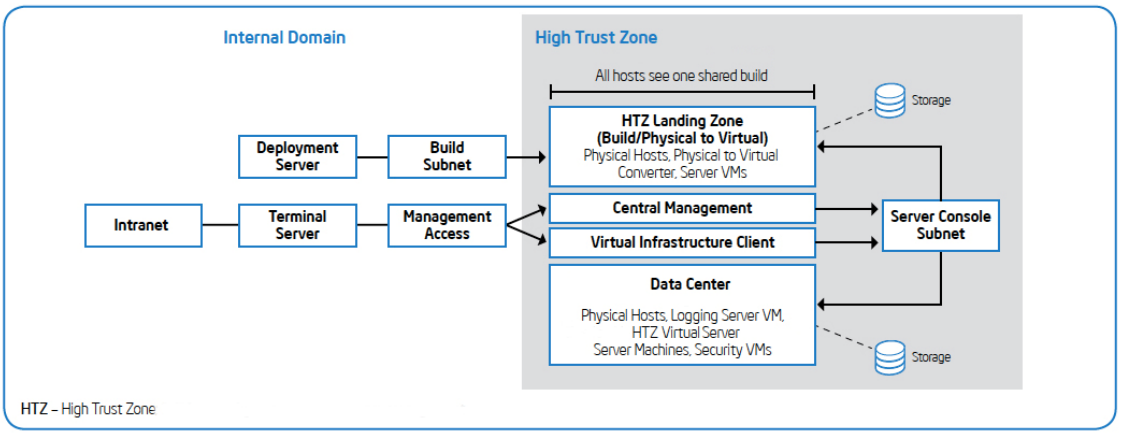

Fig. 8: Proposed Approach for building a High Trust Zone

Fig. 8 illustrates how HTZ can be used by the cloud providers to secure the VMs and the cloud infrastructure on IaaS platform by following the security in proposed two phases.

Phase -1 - Configuring the Virtualized Infrastructure

Step -1 - Securing the Virtual Cloud

The first step to protect the virtual cloud is to protect the virtualization infrastructure by isolating the infrastructure (virtualized) from the servers that are going to be virtualized, also by protecting accounts that will be used to control virtualization, securing applications by moving them to the High trust zone and by hardening the Operating System (OS). By hardening the OS, the unnecessary applications or features of the OS will be removed and only the required ones will be kept. The most important factor of this process is to isolate the virtualization infrastructure, this means that the customer VMs will not impact any of the system or data center VMs of the cloud provider. As shown in Fig. 8 the Data center zone is the one where all the necessary VMs of the data center resides whereas the HTZ landing zone where all the VMs belonging to the clients will be hosted, this ensure that all the VMs share their space accordingly and in case of any breach in HTZ layer the data center layer will be least impacted since it is already isolated and has separate storage.

Step -2 - Securing applications and moving them to High Trust zone

Before moving applications to High Trust Zone it is necessary to build a preproduction virtualized environment, this will be used to test the application (to be moved) for testing, compatibility, application review and some testing on the security perspective of the application. The goal for application testing from security perspective is to ensure that existing policies of the application or the VM is carried over from the physical world to the virtual world. For instance whether to allow the GPO (group policy objects) objects in the application such as remote deployment of application updates etc. Hence the user of the cloud should ensure that they carry the same security policy of their physical hosts on the hosted VMs, this is to ensure the safety of their VMs and being in-line with their existing enterprise security policies. If the security policies are not implemented on the VMs then this solution might not work.

Step – 3 - Risk Assessments of Applications

Risk assessment of application is mandatory to find out the risks associated with the applications before moving them to the High Trust Zone. This assessment is required to ensure that applications or the system being added to the high trust zones do not have any additional risks associated with them or add to the security risks of the High Trust Zone security environment. This assessment can also provide additional benefit of identifying the opportunity of understanding and re-examining the security risks associated with legacy applications. The following should be considered before conducting the risk assessment:

- Eliminate overlap access from outside High Trust Zone
- Evaluate the network architecture to properly define firewall rules and identifying required configurations for proxies and bastion hosts. A

bastion host is a computer on a network specially designed to withstand attacks [19].

- Understanding the security requirements of the application, such as logging capabilities of the application, the data being stored by the application, the directory permissions that the application need, authentication and security lifecycle of the application.
- Evaluating the security of the system including authentication, access control, restrictions and group policies (if any)

Phase - 2 Network Monitoring

To secure the High Trust Zone and to provide the High Trust Zones with the capability of prevention and protection environment, there is a strong need of implementing a mix of network attack and intrusion detection capabilities. At first, the network intrusion monitoring has to be implemented that will analyze and monitor all traffic coming into and going out of the high trust zone. Additionally, there is a strong need of implementing network traffic analysis behavior, this process would ensure the normal traffic patterns and shall enable abnormal traffic activity, with a facility of sending appropriate alerts.

Besides the aforesaid the authors also suggest implementing Host Based Intrusion Prevention System [20] and Host Based Intrusion Detection System specifically on the VMs deployed on the High Trust zones, this would help to have a broader and wide coverage of the attacks specifically to the VMs.

5. Conclusion

In this paper we have presented the unique security and privacy issues in cloud computing. The paper provides a thorough overview of security issues which IT decision makers need to consider before adopting a cloud service. According to the survey presented over 42% respondents place the security responsibility to the cloud service providers in SaaS adoption. Therefore, it is vital to engage senior management in discussions with regards to imposing strong security countermeasures in cloud services. Security practitioners which are 60% of the respondents believe that security policies of cloud services providers should be evaluated before deployment. Although majority of respondents from management feel confident about adopting cloud, security and network practitioners are reluctant to put a blind faith on cloud service providers. Enhancements are needed in current security solutions to fully realize the benefits of cloud computing.

For a safer Infrastructure as a Service (IaaS) a Virtualized High Trust Zone (VHTZ) is presented to secure the virtual machines in IaaS environment. The two phases VHTZ ensures the cloud security by configuring the virtualized infrastructure and ensuring network monitoring to detect and prevent network attacks. The VHTZ increases the monitoring of incoming and outgoing network traffic by providing extra host level security protection to the individual VMs by implementing Host Intrusion Detection system and Host Intrusion Prevention system at each of the VMs deployed in the High Trust Zone.

References

[1] Mansukhani, B., and Zia, T. A. (2011). An Empirical Study of Challenges in Managing the Security in Cloud Computing. 9th Australian Information Security Management Conference (secau Security Congress 2011). December 5 – 7, 2011, Perth, Australia.

[2] Mansukhani, B., and Zia, T. A. (2012). Security Challenges and Countermeasures in Cloud Computing. 10th Australian Information Security Management Conference (secau Security Congress 2012). December 3 – 5, 2012, Perth, Australia.

[3] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/csaguide.pdf

[4] Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Retrieved August 18, 2012, from World Privacy Forum: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[5] Pearson S, e. a. (2009). Scalable, Accountable Privacy Management for Large Organizations. (pp. 168-174). INSPEC: IEEE.

[6] Cavoukian , A., Taylor, S., & Abrams, M. (2010). Privacy by Design. Retrieved August 12, 2012, from Essential for Organizational Accountability and Strong Business Practices: http://www.springerlink.com/content/96852p1667mwl665/

[7] Chen , S., & Wang, C. (2010). Accountability as a Service for the Cloud: From Concept to Implementation. IEEE World Congress on Services. 6th, pp. 90-95. IEEE

[8] ENISA. (2009). Benefits, risks and recommendations for information security . Retrieved August 15, 2012, from European Network and Information Security Agency: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[9] Subramanian, K. (2009). Public v/s Private Cloud computing. Retrieved 04 02, 2011, from http://www.cloudave.com/1670/public-vs-private-cloud-brouhaha-my-take/

[10] Center, E. P. (2009). USA Patriot Act. Retrieved 07 18, 2011, from E.P.I.C. Patriout Acts: http://epic.org/privacy/terrorism/usapatriot/

[11] Winkler, V. (. (2011). Securing the Cloud - Cloud Computing Security Techniques and Tactics (1st Edition ed.). Oxford: Syngress

[12] Brodkin, J. (2008). Gatrner: Seven Cloud computing security risks. Retrieved 06 07, 2011, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[13] Grobauer, B., Walloschek, T., & Stöcker, E. (2010). Understanding Cloud-Computing Vulnerabilities. IEEE Security and Privacy (pp. 1-7). IEEE computer Society Digital Library. IEEE Computer Society

[14] Carbone, M., Zamboni, D., & Lee, W. (2008). Taming Virtualization. IEEE Security and Privacy, 6, pp. 65-67

[15] King, S., Chen, P., & Wang, Y.-M. (2006). SubVirt: Implementing malware with virtual machines. *IEEE Symposium on Security and Privacy* (pp. 314-320). IEEE

[16] Cabuk, S., Dalton, C., & Edwards, A. (2008). *A Comparative Study on Secure Network Virtualization.* Retrieved April 02, 2012, from HP Labs: http://www.hpl.hp.com/techreports/2008/HPL-2008-57.pdf

[17] Ormandy, T. (2007). An Empirical Study into the Security Exposure to Host of Hostile Virtualized Environments. *Applied Security Conference.* Canada

[18] Gutierrez, E., Kohlenberg, T., Mahankali, S., and Sunderland, B (2012). Virtualizing High-Security Servers in a Private Cloud. IT@Intel White Paper

[19] Dillard, K. (n.d.). *Intrusion Detection FAQ: What is a bastion host?* Retrieved May 2012, from SANS: http://www.sans.org/security-resources/idfaq/bastion.php

[20] Newman, R. (2009). *Computer Security: Protecting Digital Resources* (1st ed.). Jones & Bartlett Learning.

Tanveer Zia is Senior Lecturer in Computing, Course Coordinator for the Doctor of Information Technology, and Associate Head of School, School of Computing & Mathematics, Charles Sturt University, Australia. He has earned his PhD from the University of Sydney in 2008, Master of Interactive Multimedia (MIMM) from University of Technology Sydney in 2004, MBA from Preston University USA in 1997, and Bachelors of Science in Computer Sciences from Southwestern University, Philippines in 1992. Tanveer's broader research interests are in ICT security. Specifically he is interested in security of low powered mobile devices. He is also interested in biometric security, cyber security, cloud computing security, information assurance, protection against identity theft, trust management, forensic computing, and law and ethics in ICT. He is serving on Technical and Program Committees of several international conferences in his area of research. He actively publishes in international conferences, symposiums, workshops, and refereed journals.

Tanveer is a Senior Member Australian Computer Society and Certified Professional (MACS Snr CP), Senior Member Institute of Electrical and Electronics Engineers (IEEE), Senior Member International Association of Computer Sciences and Information Technology (IACSIT), Member IEEE Computer Society, Member Australian Information Security Association (AISA), Member ISACA and Academic Advocate for CSU.

Bhupesh Mansukhani is a candidate for Doctor of Information Technology at Charles Sturt University, Australia. He is studying security and privacy concerns in cloud computing and is supervised by Dr Tanveer Zia. Bhupesh earned his Master of Information Technology and Bachelor of Information Technology qualifications from Charles Sturt University in 2011 and 2004, respectively. Bhupesh has worked for IBM India as Project Manager (IT Infrastructure) and holds professional certifications such as Project Management Professional and IT Service Management. He has produced several publications in cloud computing security.